VM-Series Virtual Firewalls Secure Public Clouds, Private Clouds, and Branch Offices

Industry Context

Cloud and mobility initiatives are transforming modern organizations by giving employees and customers alike greater access to data and services anywhere, anytime. To support these new demands, organizations are turning to public cloud platforms and migrating their data centers to private clouds based on virtualization technology, such as hypervisors and software-defined networking (SDN).

Branches are also changing rapidly—most notably by replacing the corporate wide-area network (WAN) with software-defined WAN (SD-WAN) so that all branch traffic moves over the public internet. According to a recent survey, nearly half (49%) of enterprises are leveraging hybrid cloud and on-premises approaches, and more than one-third (37%) plan to shift or deploy all their workloads to the cloud.[1]

While public and private clouds undoubtedly provide organizations with the speed, agility, and scale they need, these environments also introduce myriad network security challenges that organizations did not face with traditional on-premises data centers.

VM-Series Overview

Palo Alto Networks VM-Series Virtual Next-Generation Firewalls provide all the capabilities of our physical Next-Generation Firewalls in a virtual machine (VM) form factor, delivering inline network security and threat prevention to consistently protect public and private clouds, virtualized data centers, and branch locations. The broad capabilities of the VM-Series are designed to meet today's network security challenges, giving teams the power to inspect and control inbound and outbound traffic in public cloud environments as well as define and enforce segmentation and threat prevention policies between trust zones in virtualized data centers and branches.

Key Capabilities

The VM-Series effectively addresses the security challenges of hybrid and multi-cloud environments as well as branch offices by providing deep visibility and precise control, reducing the attack surface and preventing threats, and automating network security at scale.

Network-Wide Visibility and Control Protect Applications and Data

The VM-Series protects your applications and data with next-generation security features that deliver superior visibility, precise control, and threat prevention at the application level. By deploying the VM-Series, organizations regain visibility and control over inbound, outbound, and internal (east-west) network traffic across the entire environment. As a result, security teams can define, enforce, and manage consistent security policies across on-premises environments, private and public clouds, and branch locations—all from a single management console.

Segmentation and Threat Prevention Cut Risk

These virtual firewalls help security teams mitigate risk by reducing the attack surface through segmentation and inserting threat prevention measures throughout the environment for detection and response. With the VM-Series, organizations can implement the prevention capabilities and segmentation required by regulatory compliance standards, such as PCI DSS, HIPAA, and the SWIFT Customer Security Controls Framework. Simple, comprehensive reporting provides the information necessary to streamline audits and avoid regulatory missteps.

Automated Network Security at Scale Safeguards DevOps

In modern cloud environments, effective network security must not impede development. The VM-Series integrates security provisioning into application development lifecycles and continuous integration/continuous development (CI/CD) pipelines, allowing developers to work without interruption while network security teams seamlessly implement the controls needed to keep the environment safe and compliant. The VM-Series scales automatically with your cloud infrastructure to accommodate dynamic events such as cloud bursting.

In addition to providing consistent security posture across all these environments, VM-Series virtual firewalls solve specific problems for public and private clouds as well as branch offices (see figure 1).

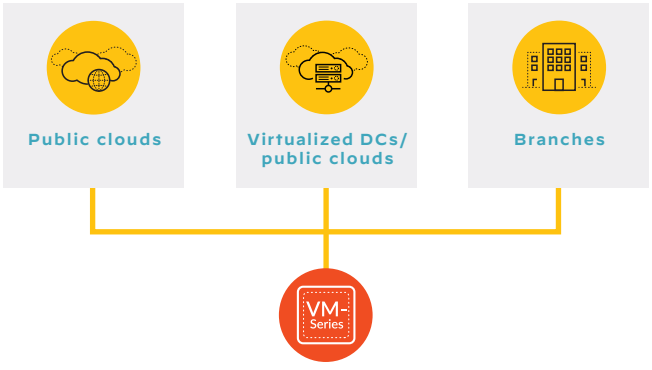

Figure 1: Consistent threat prevention and inline network security for private, hybrid, and multi-cloud environments and branch offices

[1] IDG, September 2019. https://www.infoworld.com/resources/197687/why-sd-wan-requires-a-new-approach-to-security

VM-Series in Public Cloud Environments

Application Security Detects Hard-to-Find Threats

Challenge

Port-based security groups implemented by cloud service providers (CSPs) lack application-level visibility into network traffic and have few threat prevention capabilities. As a result, native cloud security groups will not discover threats that exploit open ports (e.g., 80/443) or target vulnerabilities in non-web apps, such as the well-known ones in Apache Struts.

Solution

VM-Series firewalls inspect every inbound packet and block suspicious traffic based on application type or user identity, going beyond simple port blocking to protect traffic over open ports. The VM-Series also provides advanced security capabilities, such as intrusion prevention system (IPS) and sandboxing, to defend against both known and unknown vulnerabilities at the edge of a public cloud environment (see figure 2).

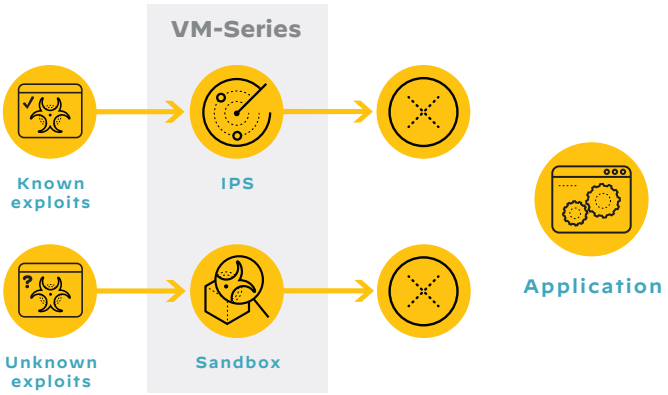

Figure 2: Integrated IPS and sandboxing to block known and unknown exploits

Outbound Traffic Protection Stops Exfiltration

Challenge

If attackers make it past perimeter controls, they still need a way to exfiltrate data from the environment. Often, they take advantage of allowed encrypted traffic flows, such as domain name system (DNS) traffic, to hide data as it leaves the environment.

Example

An attacker gains access to your environment by stealing a user's credentials. After conducting reconnaissance and identifying valuable information, the attacker executes a DNS tunneling technique to exfiltrate it from the compromised application by hiding the data in encrypted DNS traffic.

Solution

VM-Series firewalls can decrypt traffic for outbound content inspection. The DNS Security service on the VM-Series ensures that even allowed encrypted traffic flows are inspected and protected (see figure 3).

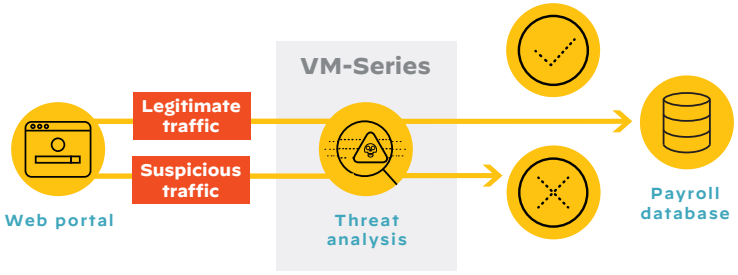

Figure 3: Prevention of lateral movement to stop attackers from accessing sensitive data

Filtering and Inspection Boost Developer Security

Challenge

Native CSP firewalls have limited capabilities to filter and inspect outbound traffic leaving the cloud environment. As a result, if developers download compromised open source code from a public code repository, they may unwittingly allow malware to penetrate the security perimeter. Once inside, threats can move laterally to locate information for exfiltration.

Solution

VM-Series firewalls provide URL Filtering to ensure that developers can only access known good repositories that are maintained and secured internally (see figure 4).

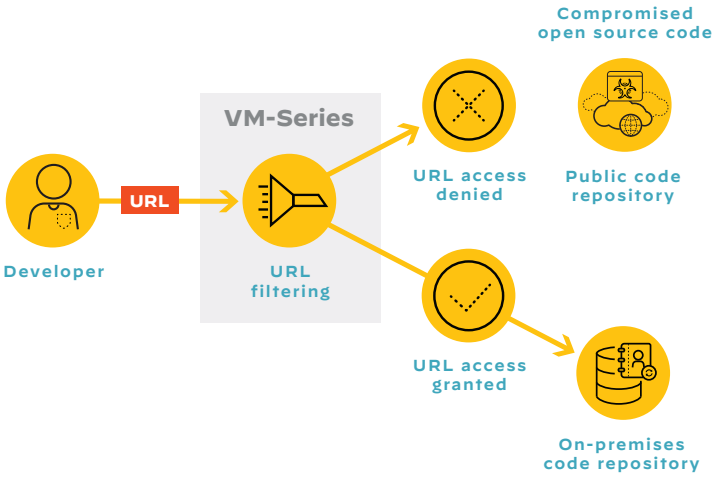

Figure 4: URL Filtering to prevent developers from accessing compromised code in a public repository

Comprehensive Control Across Multiple Clouds Makes Security Consistent

Challenge

As organizations divide application hosting between multiple public and private clouds, overall security posture becomes more fragmented and difficult to manage. Each part of the environment requires its own policy model and security controls, which increases operational complexity, creates security gaps, and causes delays for cloud migration initiatives.

Example

A large enterprise has critical applications hosted on a private cloud and two different public cloud environments. To enforce consistent security policies across all three parts of this hybrid environment, the security team must duplicate policies across three clouds using the native controls in each—a labor-intensive and error-prone task. Managing overall security posture requires the team to develop expertise in each cloud's controls and management interface.

Solution

VM-Series virtual firewalls deployed in multiple public and private cloud environments can all still be managed from the same console. This lets security teams deliver the same best-in-class security capabilities to each environment and extend a uniform policy model across the entire ecosystem to ensure consistency and simplification of overall security posture (see figure 5).

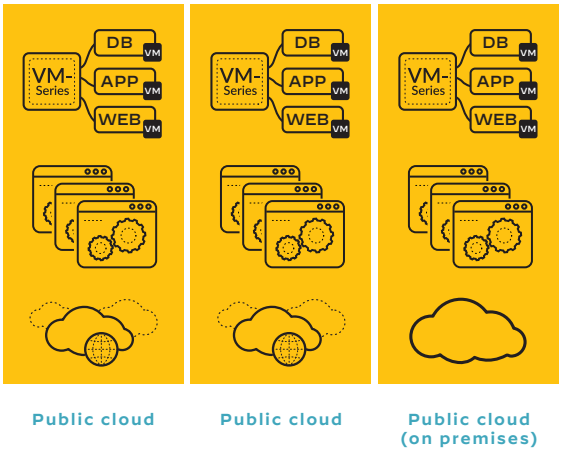

Figure 5: Consistent policy enforcement to secure public and private clouds across the full hybrid environment

VM-Series in Private Cloud Environments

As organizations transition from traditional data center architectures to private clouds, their security teams encounter challenges unique to individual use cases, such as SDN and virtual desktop infrastructure (VDI).

Segmentation and Microsegmentation Protect Against Lateral Movement

Challenge

Network security teams lack visibility and control over traffic in virtualized networks and private clouds, often leading to flat virtual networks where any workload can communicate with any other workload.

Example

An organization has decided to virtualize its primary data center to cut infrastructure costs and create a private cloud capable of delivering a public-cloud-like experience on-premises. As a result, this new highly connected environment experiences an explosion of east-west traffic between virtualized services and applications. This traffic is obscured from the network security team because it never passes through perimeter firewalls.

Solution

VM-Series firewalls deployed strategically throughout a virtualized environment create trust zones based on an organization's risk profile and tolerance level. Critical applications are placed in their own trust zones, with Threat Prevention turned on to inspect traffic to and from the application. Sensitive data subject to compliance standards is enclosed in another trust zone that enforces the security measures required for compliance.

Augment Software-Defined Networking with Threat Prevention

Challenge

Many organizations deploy SDN solutions, such as VMware NSX®, Cisco ACI®, and Nutanix Flow, to enforce microsegmentation in their virtualized environments. Each of these is a good initial step for restricting traffic, but they lack the ability to detect threats present in allowed traffic flows. Also, they become yet more tools for network security teams to manage.

Example

An organization has deployed VMware NSX in its virtualized environment to simplify networking and create microsegments for some critical applications. NSX restricts workload communication to only the traffic necessary for the applications to function. However, in addition to accessing shared databases, the applications leverage DNS and other shared services as part of their normal operations. An attacker can use these allowed connections to move laterally or exfiltrate information from the environment.

Solution

VM-Series virtual firewalls seamlessly integrate with VMware NSX, Cisco ACI, Nutanix Flow, and other SDN solutions to allow the rapid and accurate insertion of advanced security services, such as IPS or DNS Security, between microsegments to inspect and protect allowed traffic. A security team can manage its entire policy model, as well as any virtual firewalls deployed in public clouds, from the same interface as the organization's hardware firewalls (see figure 6).

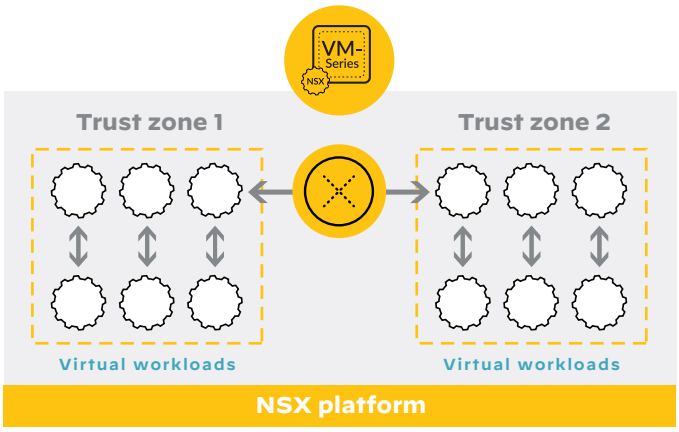

Figure 6: Integration with SDN tools to augment microsegmentation with threat prevention and protect workload-to-workload interactions between trust zones

VDI Security Meets Threats to Remote and Distributed Workforces

VDI deployments offer a host of operational efficiencies. They also present challenges for network security teams that lack visibility and control over their VDI traffic, however, because attacks entering the network via VDI devices can move laterally to threaten other high-value data center assets.

Example

An organization deploys VDI, which brings all endpoints into the primary data center. Because end users control these internet-connected machines, the VDI devices have a low trust level and must be segmented from the rest of the data center environment. Any allowed traffic to shared services or applications in the data center must be inspected for threats.

Solution

VM-Series virtual firewalls deployed at the edge of the VDI environment ensure that virtual desktops are properly segmented and traffic is inspected appropriately (see figure 7).

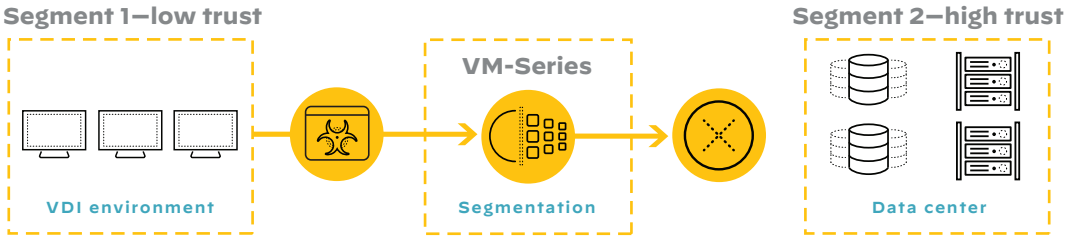

Figure 7: Segmentation and threat prevention capabilities to protect data center assets from attacks originating in the VDI environment

VM-Series in Branch Offices

Geographically dispersed organizations are embracing digital transformation for their branch offices and retail locations, creating software-defined branches. VM-Series firewalls are ideal to help these organizations enforce segmentation in their branches and use secure SD-WAN for branch connectivity.

Local Branch Segmentation Helps with Compliance

Challenge

Often, network security teams must enforce segmentation and threat prevention policies between sensitive applications and data as well as the rest of the branch network to achieve compliance.

Example

A retail chain lacks personnel with the expertise to enforce IPS and local segmentation between its point-of-sale systems and the rest of the network in all stores, but these are required for PCI DSS compliance. To add to the problem, the retail locations are tight on space, making it difficult to install physical firewalls.

Solution

VM-Series virtual firewalls can be deployed on existing servers in the stores, avoiding the need for additional hardware. This allows security teams to create a single security policy to enforce required segmentation and intrusion prevention to protect PCI-relevant data. The organization can manage its branch security centrally, using the same management console that controls security for its data center and public cloud network (see figure 8).

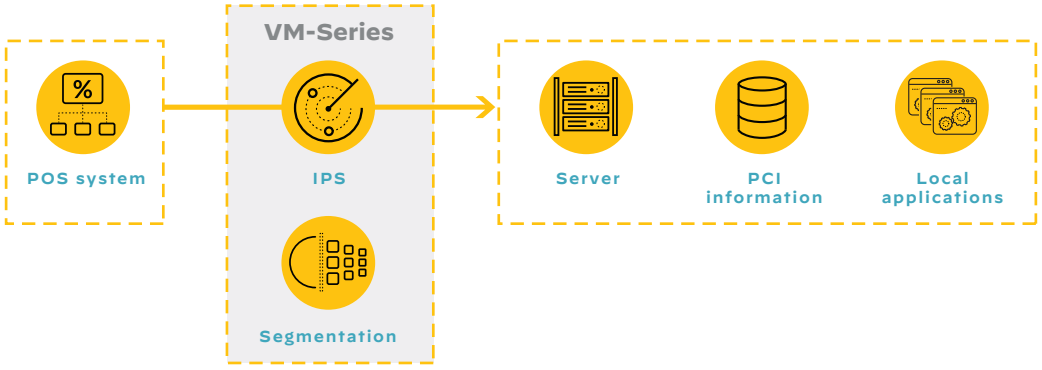

Figure 8: Support for compliance frameworks (e.g., PCI DSS) with IPS, segmentation, and other security features

Software-Based Perimeter Security Simplifies Deployment

Challenge

With the growing adoption of software as a service (SaaS) and other remote services, many organizations are turning to software-defined branch strategies. They embrace technologies such as SD-WAN to simplify networking and reduce the amount of hardware branch locations need. Traditional hardware firewalls are bulky and require on-site expertise to deploy and configure, but branches often lack local technical expertise and extra space for hardware.

Example

A retail organization has more than 1,000 stores worldwide, each with a hardware firewall installed. The company wants to move to a software-defined branch model to save space and provide centralized IT control, but doesn't want to sacrifice branch security.

Solution

VM-Series virtual firewalls replace hardware firewalls and deliver the same level of perimeter security. As virtual machines, they can be deployed on existing servers, alleviating the need to ship, install, and maintain hardware firewalls. VM-Series firewalls can also deliver SD-WAN to further consolidate branch connectivity and security (see figure 9).

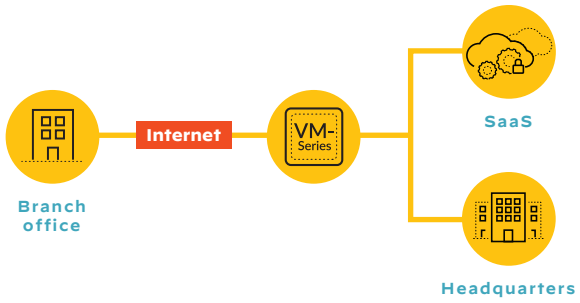

Figure 9: Perimeter deployment to protect the branch from internet-based threats

Secure SD-WAN Increases Performance and Network ROI

Challenge

As the number of applications hosted in clouds and distributed organizations grows, traditional networks and WANs become less and less able to effectively manage networks and security. Leveraging legacy connectivity options such as multiprotocol layer switching (MPLS) in the data center is not effective in today's cloud-connected world.

Example

A retail organization is suffering from poor network performance in its stores because of the way security is enforced: traffic is continually backhauled to the core data center before it is sent to the public cloud. This configuration also increases bandwidth costs.

Solution

VM-Series virtual firewalls can be used to build a hub-and-spoke SD-WAN deployment between store locations, the core data center, public cloud environments, and SaaS applications. For small or regional deployments, VM-Series firewalls can run SD-WAN in a mesh architecture, connecting to each other without the need for a hub (see figure 10).

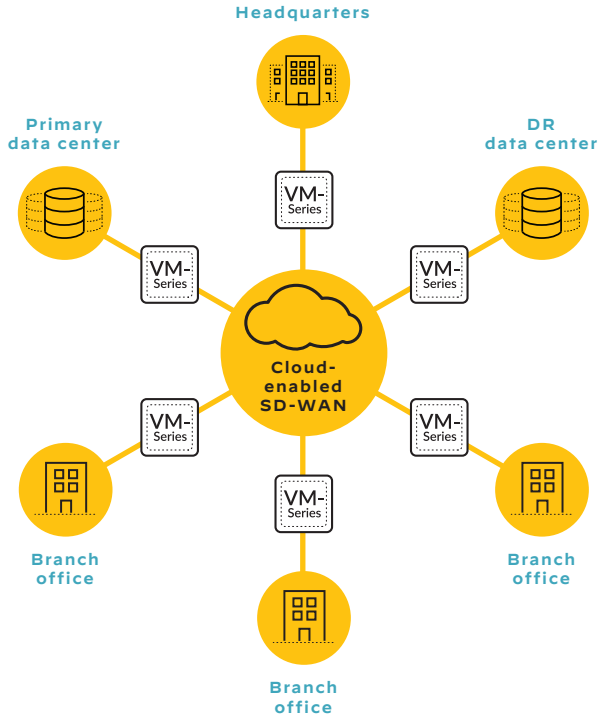

Figure 10: VM-Series virtual firewalls in a hub-and-spoke architecture

VM-Series in Branch Offices

Palo Alto Networks VM-Series differ from other virtual firewalls in four areas critical for network security teams.

1. Elastic and Scalable Deployment Meets Actual Needs

VM-Series virtual firewalls meet real-world demand with flexible pricing and features designed for deployment and configuration at scale: auto-scale templates, bootstrapping, and other automated capabilities. VM-Series firewalls can even be deprecated after demand has subsided, helping organizations avoid paying for unnecessary services.

2. Automated Orchestration Provides Security at DevOps Speed

Integration with automation and orchestration platforms, such as Terraform® and Ansible®, allows VM-Series firewalls to be deployed as part of the application development process to ensure security at DevOps speed. A tag-based policy model, tight integration across myriad cloud infrastructure providers, and a fully documented XML API allow you to create flexible policies that can adapt to ever-changing environments, regardless of the underlying infrastructure.

3. Operational Simplicity Alleviates the Need for Multiple Products

Unified management through Panorama™ network security management simplifies network security oversight, even across different infrastructures and clouds. A single policy model across on-premises deployments, private and public clouds, and branches reduces gaps in the overall security posture. Advanced security services deployable on any Palo Alto Networks firewall form factor reduce the need for additional point security products, further decrease complexity, and make it easy to deploy the right security controls wherever needed in your environment.

4. Best-in-Class Security Helps Ensure Ongoing Operations

Palo Alto Networks has been a Leader in the Gartner Magic Quadrant® for Network Firewalls (formerly "Enterprise Network Firewalls") eight consecutive times. Our firewalls and advanced security services protect more than 70,000 organizations worldwide, ranging from enterprises and governments to hospitals and schools.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com